



COPY

For : The Patent Application

Our Ref. : NT0226US

● LIST OF THE PRIOR ART REFERENCES CITED IN THE SPECIFICATION

1. Advances in Cryptology-CRYPTO etc.
2. The Chain & Sum Primitive and Its Applications to MACs
And Stream Ciphers
Mariusz H. Jakubowski and Ramarathnam Venkatesan
(281-293)
"Advances in Cryptology CRYPTO'98" Kaisa Nyberg (Ed.)
3. Keying Hash Functions for Message Authentication
Mihir Bellare and Ran Canetti and Hugo Krawczyk (1-328)
"Advances in Cryptology CRYPTO'96" Neal Koblitz (Ed.)
4. An Integrity Check Value Algorithm for Stream Ciphers
Richard Taylor (40-48)
"Advances in Cryptology CRYPTO'93" Douglas R. Stinson (Ed.)
5. Algorithm Types and Modes (189-401)
6. UMAC: Fast and Secure Message Authentication
J. Black, S. Halevi, H. Krawczyk, T. Krovetz, and P. Rogaway
(pg. 216-269)
"Advances in Cryptology CRYPTO'99" Michael Wiener (Ed.)
7. MMH: Software Message Authentication in the Gbit/Second
Rates Shai Halevi and Hugo Krawczyk (172-189)
"Fast Software Encryption" Eli Biham (Ed.)

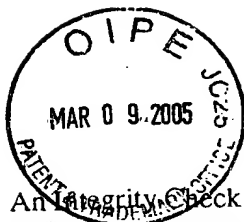
8. Integrity-Aware PCBC Encryption Schemes

Virgil D Gligor, Pompiliu Donescu (1-13)

"The 1999 Security Protocols Workshop Pre-proceedings"

9. Stream ciphers based on LFSRs (203-369)

Reference



Richard Taylor	An Integrity Check Value Algorithm for Stream	pp.40-48	LNCS773	CRYPTO93
Mihir Bellare	Keying Hash Functions for Message Authentication	pp.1-15		CRYPTO96
Ran Canetti	Universal Hashing and Multiple Authentication	pp.16-30	LNCS1109	CRYPTO96
Hugo Krawczyk	Universal Hash Functions from Exponential Sums over Finite Fields and On Fast and Provably Secure Message Authentication Based on The Chain & Sum Primitive and Its Applications to MACs and Stream Ciphers	pp.31-44	LNCS1109	CRYPTO96
M. Atici		pp.313-328	LNCS1109	CRYPTO96
D. R. Stinson		pp.281-293	LNCS1403	EUROCRYPT98
Tor Helleseht	UMAC: Fast and Secure Message Authentication	pp.216-233	LNCS1666	CRYPTO99
Thomas Johansson	Square Hash: Fast Message Authentication via Optimized Universal Hash Constructing VIL-MACs from FIL-MACs: Message Authentication under Weakened Assumptions	pp.234-251	LNCS1666	CRYPTO99
Victor Shoup	MMH: Software Message Authentication in the Gbit/Second Rates	pp.252-269	LNCS1666	CRYPTO99
Mariusz H. Jakubowski		pp.172-189	LNCS1267	FSE97
Ramarathnam Venkatesan				
J Black				
S. Halevi				
H. Krawczyk				
T. Krovetz				
P. Rogaway				
Mark Etzel				
Sarvar Patel				
Zulfikar Ramzan				
Jee Hea An				
Mihir Bellare				
Shai Halevi				
Hugo Krawczyk				
Virgil D. Gligor	Integrity-Aware PCBC Encryption Schemes			The 1999 Security Protocols Workshop Pre-proceedings, Cambridge UK, 1999.
Pompiliu Donescu		pp.203-212, 250-259, 263-266, 347-349, 352-		
Alfred J. Menezes	Handbook of Applied Cryptography	pp.189-209, 398-	ISBN0-8493-8523-7	
Paul C. van Oorschot				
Scott A. Vanstone				
Bruce Schneier	Applied Cryptography, second edition		ISBN0-471-11709-9	